ANNEX L (OPERATIONS SECURITY) to TRADOC Mobilization and Operations Planning and Execution System 1-97 (TMOPES 1-97)

REFERENCES:

JCS Pub 18, Policy, Concept and Standards for Operations Security.
JCS, Operations Security Survey Planning Guide.
AR 530-1, Operations Security.
TRADOC Pam 525-6, Operations Security - Doctrinal Guidelines for Tactical Units and Trainers.

1. SITUATION.

a. Enemy Forces. See ANNEX B, Intelligence.

(1) Signal Intelligence (SIGINT). The SIGINT threat is present in the capability to monitor wire and radio traffic on unsecure nets. The most critical risks to the security of operational information are the commercial telephone system and voice radio telecommunications. TRADOC uses these methods of communication daily for transmitting UNCLASSIFIED information relating to military operations, plans, weaknesses, strengths, special projects, and ongoing support to all levels of mobilization.

(2) Human Intelligence (HUMINT). The HUMINT threat is present. Espionage agents develop accurate and timely data concerning forces; their location, deployment, posture, and capabilities. HUMINT threats are present in the information available from the local population.

(3) Electronic Warfare (EW). EW is a threat to operations in that two techniques can result in compromise of data. Jamming creates confusion and disorder by breaking down normal communications channels, thereby revealing alternate frequencies or forcing communications into less secure modes. Electronic deception destabilizes various electronic means of communications by altering or simulating friendly electromagnetic emissions.

(4) Imagery. The growing capability of imagery, obtained by satellites, aircraft, and other Photo Intelligence (PHOTINT) platforms, presents a substantial challenge to deny information to any potential enemy, and increase the difficulty of successful deception.

(5) Open Literature. A potential hostile enemy can exploit news media and technical publications. This threat is the most difficult to control and divulges information as to

operations level and success of any level of mobilization. Military communications that are normally UNCLASSIFIED, such as weather and flight plan traffic, obtained by overt means, also furnish an opportunity for hostile intelligence.

b. (U) ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI). The following EEFI are applicable at all levels of command. Use the information as a guide to develop supporting EEFI plan.

	PROTECTION REQUIRED DURING			
SUBJECT REQUIRING PROTECTION	PLAN PHASE	PREP PHASE	EXEC PHASE	POST PHASE
1. Locations, defenses, and/ or vulnerability of key U.S. HQ, communications centers, logistics depots, and alternate headquarters.	X	X	X	X
2. Identification, strength, and readiness of augmentation forces available for immediate deployment/employment.		X	X	
3. Capability of augmentation forces to support sustained mobilization operations.		X	X	X
4. Time to commence effective mobilization operations.		X	X	
5. Long-haul communications support which is unique to the operation.		X	X	
6. Locations, techniques, capabilities, limitations, and effectiveness of supporting SIGINT and ELINT programs.	X	X	X	X
7. Structure, location capabilities and limitations of U.S. intelligence collection resources.	X	X	X	X
8. U.S. intelligence collection requirements and PIRs.	X	X	X	X

9. Effects of enemy military activities and operations on U.S. command and control systems	X	X	X	X

	PROTECTION REQUIRED DURING			
SUBJECT REQUIRING	PLAN	PREP	EXEC	POST
PROTECTION	PHASE	PHASE	PHASE	PHASE
and logistics.				
10. Vulnerability of U.S. installations to sabotage and penetration.	X	X	X	X
11. Vulnerability of TRADOC installations to air and missile attack.	X	X	X	X
12. Area of primary responsibility for U.S. forces.		X	X	
13. Evacuation of U.S. nationals and selected liens.		X	X	X
14. Military assistance in support of evacuation of U.S. nationals and selected aliens.		X	X	
15. Deception objections, stories, and methods.	X	X	X	X
16. Counterintelligence operations for identifying and neutralizing enemy espionage, sabotage, and subversive activities.	X	X	X	X
17. All aircraft/ship operating locations.	X	X		X
18. All aircraft operating capabilities.	X	X	X	X
19. Characteristics, capabilities and limitations of U.S. offensive and defensive weapons and systems.	X	X	X	X
20. Training base expansion	X	X	X	X

	PROTECTION REQUIRED DURING			
SUBJECT REQUIRING PROTECTION	PLAN PHASE	PREP PHASE	EXEC PHASE	POST PHASE
limitations/deficiencies.				
21. MOBSTA troop lists.	X	X	X	X
22. POE/POD.	X	X	X	X
23. CONUS moves.	X	X	X	X
24. Consolidated unit listings	X	X	X	X

c. Friendly Forces. (See basic plan)

d. Assumptions. (See basic plan)

2. MISSION: On order, TRADOC employs operations security (OPSEC) during all phases of support to operations, contingencies and levels of mobilization, to deny potential enemies sensitive information.

3. EXECUTION.

a. General.

(1) Definition. Operations Security (OPSEC) actions protect military operations and activities from compromise by identifying and subsequently eliminating or controlling intelligence indicators susceptible to hostile exploitation. Operations encompasses all activities of Army organizations, including; mobilization, deployment, administration, personnel, intelligence, security, communications-electronics, planning, training, operating, logistics, and civil-military functions.

(2) OPSEC objective. Preserve the advantage of surprise and enhance the probability of successfully accomplishing the mission. "Security" in this context relates to protecting friendly forces from surprise attack by the enemy and using the elements of surprise against the enemy. Security includes activities that protect operational information and prevent the enemy from using successful countermeasures, organizing prior knowledge, or obtaining prior knowledge of friendly operations. OPSEC pervades the entire planning process and remains a continuing concern throughout the operations and during critiques, reports, press releases in the post-operation phase.

b. Tasks. HQ TRADOC and subordinate commands and installations:

(1) Implement plans and procedures IAW OPSEC directives (JCS Pub 18, AR 530-1).

(2) Develop appropriate/applicable EEFI.

(3) Develop and implement countermeasures appropriate for the threat and EEFI.

(4) Brief personnel on the threat and EEFI.

(5) Task supporting physical security, signal, security, and counterintelligence organizations to monitor operations to identify OPSEC weaknesses, assess the impact that any security breaches could have on the execution of operations, assess the possible compromise of plans, and recommend corrective action.

(6) Brief units at the Mobilization Station (MS) about local threat and countermeasures upon arrival to the MS.

(7) Integrate OPSEC awareness into the training schedules of mobilizing and deploying units.

4. ADMINISTRATION AND LOGISTICS. (See basic plan).

5. COMMAND AND SIGNAL. (See basic plan).

HARTZOG
GEN

OFFICIAL:

BAKER
Director, Operations